방송융합 서비스 개방화에 따른 보안대책 연구

정찬석*, 이명렬**,신용태*
*숭실대학교 컴퓨터공학과
**숭실대학교 컴퓨터공학과
e-mail: izmit70@gmail.com

Security Measures for the Open Convergence Service on broadcasting and telecommunication

Chansuk Jung*, MyoungYeal Lee**, Yongtae Shin*,
*Dept of Computer Engineering, Soongsil University
**Dept of Computer Engineering, Soongsil University

요 약

최근 인터넷 기술의 발전과 폭발적인 인기를 누리고 있는 스마트폰 등의 인프라요소의 발전으로 인해 방송 및 통신 서비스의 융합된 형태인 IPTV, 스마트 TV 등의 새로운 형태의 서비스가 도입되어 시장을 형성하고 있다. 이러한 새로운 형태의 서비스는 기존 몇몇의 콘텐츠 제공자가 제공하는 서비스 뿐만아니라, 자신들이 만들 콘텐츠를 이용하고자하는 프로슈머들의 욕구 또한 충족시켜주어야 한다. 이러한 서비스 시장의 변화는 기존 폐쇄적인 서비스 운영형태를 가지고 있던 사업자들의 개방화 정책을 유도하고 있다.

우리나라의 서비스 사업자들오 이러한 서비스변화에 말맞추어 개방화 전략을 앞다투어 발표하고, 새로운 형태의 서비스를 통한 시장 점유율 향상을 위해 노력하고 있다. 하지만, 개방화된 서비스 형태는 자칫 새로운 보안문제를 야기할 수 있고, 이로 인해 새로운 서비스 조기정착과 서비스 시장확대라는 목적을 저해시킬 수 있다.

이에, 본 논문에서는 방송융합서비스의 개방화 정책에 따른 새로운 서비스 형태를 알아보고, 신규서비스에 내재되어 있는 보안위협을 도출, 이에 대한 대응방안을 제시하고자 한다. 이러한 대응방안은 신규 융합서비스 안정적 도입 및 확산을 위한 기반이 될 수 있을 것이다.

1. 서 론

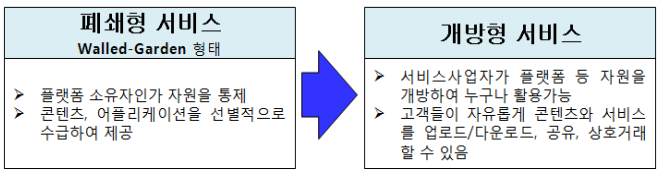
최근 스마트폰 보급의 증가와 함께, 다양한 어플리케이션을 사용할 수 있는 앱스토어 또한 폭발적인 성공을 거두고 있다. 이러한 스마트 단말기의 앱스토어의 성공을 벤치마킹하여 기존 존 Walled-Garden 형태의 서비스를 제공하던 국내 KT, SKB, LGU+ 등의 IPTV 사업자와 스마트 TV를 생상보급하는 삼성전자 등이 2010년도부터 본격적으로 자신들의 플랫폼과 서비스 환경을 개방화하여 더욱 많은 콘텐츠를 확보하고자 하고 있다. 이러한 움직임은 사업자들이 인터넷과 모바일에 익숙한 IT 서비스 유저들을 TV시장에 편입하여 많은 콘텐츠 확보하고 이를 통해 궁극적으로는 자신들의 시장 점유율을 증가하고자 하기 때문이다.

하지만, 기존 폐쇄되었던 플랫폼과 프로그램 개발 도구 등을 일반에게 개방하고, 서비스 런칭 또한 제공형태의 서비스로 인해 보안상의 발생 가능한 취약점에 대한 검토가 필요하다. 본 논문에서는 IPTV서비스의 개방화 정책을 다시 한번 살펴보고, 이에 따른 보안 취약점을 살펴보기로 한다.

2. 방송융합 서비스 개방화

2.1 방송융합서비스 개방화 개념

서비스 개방화란, 아래 (그림1)과 같이 기존 Walled-Garden 형태의 서비스 제공방식을 플랫폼 및 네트워크 자원을 개방하여, 누구든지 자유롭게 콘텐츠와 서비스를 제작, 이용할 수 제공하는 서비스 제공방식을 말한다.

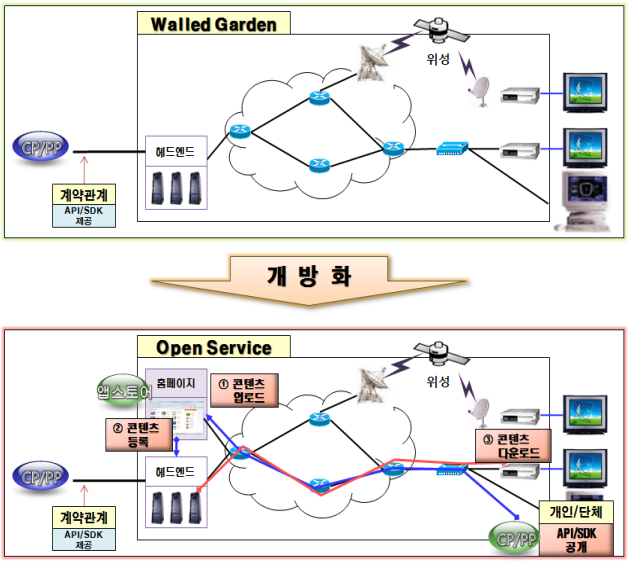


(그림 1) 개방화 서비스 개념

즉, 자사의 플랫폼을 활용하여 자유로운 콘텐츠 및 서비스 개발하고, 이를 통한 서비스 이용활성화를 추구하는 것을 말한다.
이러한 개방화를 위한 IPTV 사업자와 스마트TV 사업자들은 자사환경에 맞는 콘텐츠 저작도구(SDK[1]) 등을 공개하고 있고, 자신들의 고객이 직접 콘텐츠

를 제작하여 자유롭게 사용할 수 있는 환경을 제공하고 있다. 이러한 변화는 IT서비스 사용자들의 프로슈머화 되어 가는 현상을 반영하여 자신들의 서비스를 활성화 하고자 하는 전략이 숨어 있는 것이다.

아래 (그림 2)는 개방화 서비스를 제공하는 사업자의 서비스 형태의 변화를 나타내는 그림이다. 기존 서비스사업자과 별도의 계약이 성립된 콘텐츠 제공사업자의 콘텐츠만 활용하던 방식을 사전 등록된 사용자들에게도 콘텐츠 제공권을 주거나, 자신들이 운영하는 앱스토어 홈페이지를 통한 업로드신청을 하는 사용자 콘텐츠를 헤드엔트 시스템에 업로드해 주는 방식을 모두 적용하고 있다.



(그림 2) 개방화 서비스 구조도

2.2 주요 서비스 유형

방송융합서비스 개방화로 인해 새로 발생하는 서비스 유형은 아래 [표 1]과 같다. 채널사용에 대한 개방화, VoD 서비스 제공에 대한 개방화 TV용 앱스토어를 통한 VoD, 게임 등의 다양한 앱의 거래 등의 서비스가 신규로 생성된다. 이러한 서비스 유형의 특징 중, 가장 중요한 것은 콘텐츠 소비자인 일반 서비스 유저들이 자신들의 콘텐츠를 제작하여 올리는 프로슈머 형태로의 진화를 반영하고 있다는 것이다.

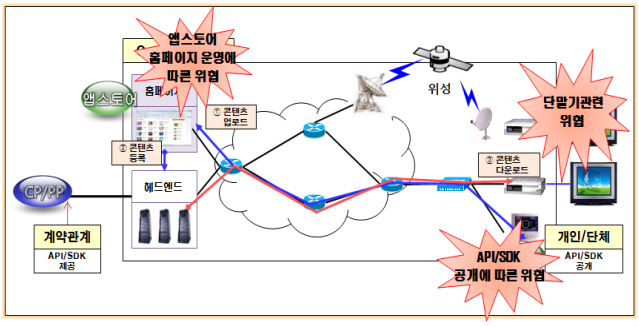
[표 2] 주요 개방화 서비스 유형

유형	내 용
채널 오픈	○ 채널 송출 권한을 가진 누구나 IPTV 등에 콘텐츠 송출 가능
VoD 오픈	○ VOD 서비스 가능한 콘텐츠를 보유했다면 누구나 IPTV로 제공 가능
TV 앱스토어	○ 애플앱스토아와 같이 TV용 어플을 개발하여 앱스토어에서 거래
개방형 CUG	○ 웹을 통해 CUG 개설/변경 가능 ○ 기업/단체가 보유한 영상을 웹에 등록해 TV로 시청
SNS	○ 개인 콘텐츠를 담을 수 있는 TV속 블로그, 싸이월드 등
Open 커머스	○ 시간과 채널의 제약없는 TV만의 특화된 오픈마켓
개방형 UCC	○ 홈페이지에 UCC를 올리고 TV로 감상

3. 방송융합 서비스 개방화에 따른 보안위협

3.1 신규 보안위협의 발생

방송융합 서비스 개방화 특성에 따라 새로이 발생되는 보안 위협은 아래 (그림 3)과 같다. 우선 개방화 서비스 플랫폼을 활용할 수 있도록 자신들의 플랫폼에 접근가능하도록 제공하는 저작도구의 취약점과, API의 취약점을 악용한 보안위협을 들 수 있다. 둘째로는 사용자에게 제공하는 앱스토어 홈페이지의 웹 취약점을 악용하여 내부 시스템에 접속하여 방송헤드엔드 시스템을 2차로 공격하는 앱스토어를 통한 침해위협을 들 수 있다. 마지막으로 방송융합 서비스를 이용하는 단말기인 셋톱박스, 스마트 TV 등의 운영체계 혹은 응용프로그램의 취약점을 악용한 침해위협이 있을 수 있다.



(그림 3) 방송 융합서비스 보안위협 개념도

물론 이외에도 인터넷기반의 서비스를 활용하는 방송융합서비스임으로 기존 인터넷에 존재하고 있는

1) SDK(Software Development Kit) : 소프트웨어 개발 도구로 소프트웨어 프레임워크, 하드웨어 플랫폼, 운영 체제 등을 위한 응용 프로그램을 만들 수 있게 하는 개발 도구의 집합

보안위협을 상속받는 것은 자명하다고 볼 수 있다. 즉, 인터넷망을 기반으로 하는 방송융합서비스는 기존 인터넷망의 침해위협과 신규 서비스 특성에 따른 새로운 보안위협을 모두 내재하고 있다고 볼 수 있다. 기존 인터넷 망에 사용에 따른 보안위협은 제외하고 방송융합 서비스의 특성에 따라 새로이 발생하는 보안위협은 아래표와 같이 세분화할 수 있다.

보안위협	세부위협 명칭
SDK, API 관련 위협	① 개발환경 SDK의 S/W취약점을 악용한 공격
	② SDK를 이용하여 숨겨진 코드를 메모리상에 덤프하여 알아내어 이를 악용한 침해시도
	③ SDK 함수를 활용 비인가 영역 접근 시도
	④ SDK 디버깅 도구를 통해 특정 메모리영역 접근 및 정보획득
	⑤ SDK에 사용될 Security모듈의 취약점 악용
앱스토어 운영에 관한 위협	① 앱스토어 홈피를 통한 악성코드 유포
	② 앱스토어 웹 사이트 공격
단말기 (셋톱박스, 스마트 TV)	① 방송융합 단말기 운영체계 취약점
	② 방송융합 단말기 악용 DoS 공격

4. 방송융합 서비스 개방화 보안위협 대응방안

첫 번째로, 플랫폼 개방(SDK 등)에 따른 정보보호 위협에 따른 대응 방안은 다음과 같다. 콘텐츠 제작을 위해 지원하는 저작도구(SDK 등) 및 라이브러리 자체에 내재된 정보보호 위협의 상속 가능성 존재한다. 즉, 저작도구(SDK 등) 및 라이브러리를 이용한 콘텐츠에 악성코드 삽입 등으로 인한 정보유출, 셋톱박스에 유해프로그램 감염으로 좀비화 등 위협 발생 가능성 존재할 수 있다. 이러한 위협에 대한 대응방안으로는 플랫폼(SDK 등)에 내재된 취약점, SDK 구조에 따라 발생 가능한 보안취약점 등 소프트웨어적인 보안위협을 사전에 분석하고, 콘텐츠 개발 환경(자바, C언더 등)에 알려진 보안 취약점을 제거하여 보급하는 것이 중요한다.

두 번째로, TV 앱스토어 관련 정보보호 위협 및 대응방안을 살펴본다. TV 앱스토어를 통한 악성코드 유포 및 앱스토어 사이트 해킹을 통한 콘텐츠 및 사용자 정보 유출 가능성 존재함으로, 콘텐츠 업로드시 악성코드 사전분석 및 콘텐츠 심의절차 마련, TV 앱스토어 싸이트 보호를 위해 홈페이지 해킹방지 대책 마련하여 앱스토어를 통해 발생할 수 있는 다양한 보안위협을 대처할 수 있을 것이다.

마지막으로, 셋톱박스, 스마트 TV등 단말기 지능화로 인한 정보보호 위협 및 대응방안을 알아본다. TV 앱스토어에서 다운로드 받은 콘텐츠 인스톨 등을 위해 확대된 운영체계 서비스(Http, Ftp 등)으로 인한 취약점 발생 가능하고, 시스템 해킹, 앱스토어를 통한 악성코드 감염 등으로 인한 셋톱박스 및 스마트 TV의 좀비화로 단말기를 통한 인터넷망의 DDoS 공격발생 가능하다. 이러런 보안위협을 사전에 방지하기 위해서는 셋톱박스 및 스마트 TV 운영체계 취약점 주기적인 점검 및 패치 수행하고, 단말기에서 실행되는 프로그램에 대한 화이트리스트 등을 활용 실행 프로그램에 대한 인스톨 등의 사전차단하는 등의 보안 대책을 적용하는 것이 필요하다.

5. 결론

인터넷 기술의 급속한 발전, 스마트 TV 등 지능형 단말기의 보급 확대 등과 자신이 만든 콘텐츠를 활용하고자하는 새로운 프로슈머 고객의 등장으로 인해 기존 대규모 서비스 사업자에 의해서 통제되었던 방송서비스가 통신서비스와 융합화되고, 개방화되고 있다. 이러한 방송융합서비스의 개방화는 많은 사람들의 서비스 콘텐츠 개발에 참여할 수 있는 장점이 있으나, 서비스 안전성 측면에서 보면 개방화에 따라 보급하는 콘텐츠 저작도구를 악용한 침해위협, TV 앱스토어를 통한 침해위협, 그리고 지능화된 단말기의 통한 침해위협 등 새로운 형태의 보안위협을 야기할 수 있다.

이에 본 논문에서는 방송융합서비스의 새로운 보안위협을 분석하고 이에 대한 보안대책을 제시하였다. 이러한 보안대책을 통한 방송융합서비스의 대규모 보안위협을 사전에 방지하여 서비스의 안정적 보급과 활성화에 기여할 것이다.

[참고문헌]

[1] 김진형, 황준, “IPTV 방송 기술 동향 및 전망”, 한국 인터넷 정보학회 제8권 제1호, 2007.3

[2] 전파연구소, “방송통신 융합연구 보고서”, 방송통신위원회, pp.35, 2010

[3] 강도현, “방송통신 융합서비스 활성화 방안”, 코디마, pp.44, Aug 2010

[4] 강석철, “방송통신융합서비스 보안위협 및 대응방안 연구”, 정보보호학회 논문지 제21권 제7호. pp18-22, 2011.

[5] 나재훈, “IPTV 컨버전스 환경에서 콘텐츠 보안 기술 동향”, 정보보호학회논문지 제19권 제3호, pp18-21. 2009.

[6] 위유경, “스마트워크환경에서 활용가능한 스마트 TV 기술 동향 및 보안 취약점 분석”, 한국멀티미티어 학회 춘계학술대회논문집 제15권 제1호, pp.76-79. 2012.

[7] 김대진, “스마트TV 현황 및 발전방향”, 방송공학회지, 제15권 제3호, pp122-131, 2010

[8] www.tv.qook.co.kr

[9] apps.samsung.com

[10] www.oipf.tv